The Standards People

Remote Identification and Verification Methods under eIDAS

ENISA TSP DAY - 22/09/2020

STF 588 identity proofing

Presented by: **Sylvie Lacroix – ETSI / ESI STF 588**

STF 588 - rationales

- The current European standards published by ETSI on trust services specify identity proofing only by generic requirements like “physical presence” or “means which provide equivalent assurance as physical presence”.
  - Physical presence as a benchmark is not well-defined as no requirements are posed neither for the quality of physical identity documents nor for the competence or procedures to be carried out by the person performing the check.
  - What constitutes equivalent assurance as physical presence is up to subjective judgement.
  - Guidelines for remote identity proofing are needed to avoid cumbersome and expensive physical presence procedures when possible.
- These initial rationales becomes even more pertinent under the options to review the eIDAS Regulation

STF 588 deliverables (1)

- Detail on team & project on web page: https://portal.etsi.org/STF/STFs/STF-HomePages/STF588

- **ETSI TR 119 460 Electronic Signature and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects. (18/12/2020)**

This document surveys the technologies, legislations, specifications, guidelines and standards related to or used for identity proofing. Information will then be gathered from stakeholders such as national agencies developing requirements, product and service vendors, research and academic environments, and relevant existing specifications.

- Analyse work – some figures:
  - 44 documents (or series of documents) analysed in depth through reading sheets
  - A couple of documents analysed but considered out of scope
  - In-depth responses to questionnaires: 5 from QTSPs and 9 from vendors

STF 588 – Deliverables (2)

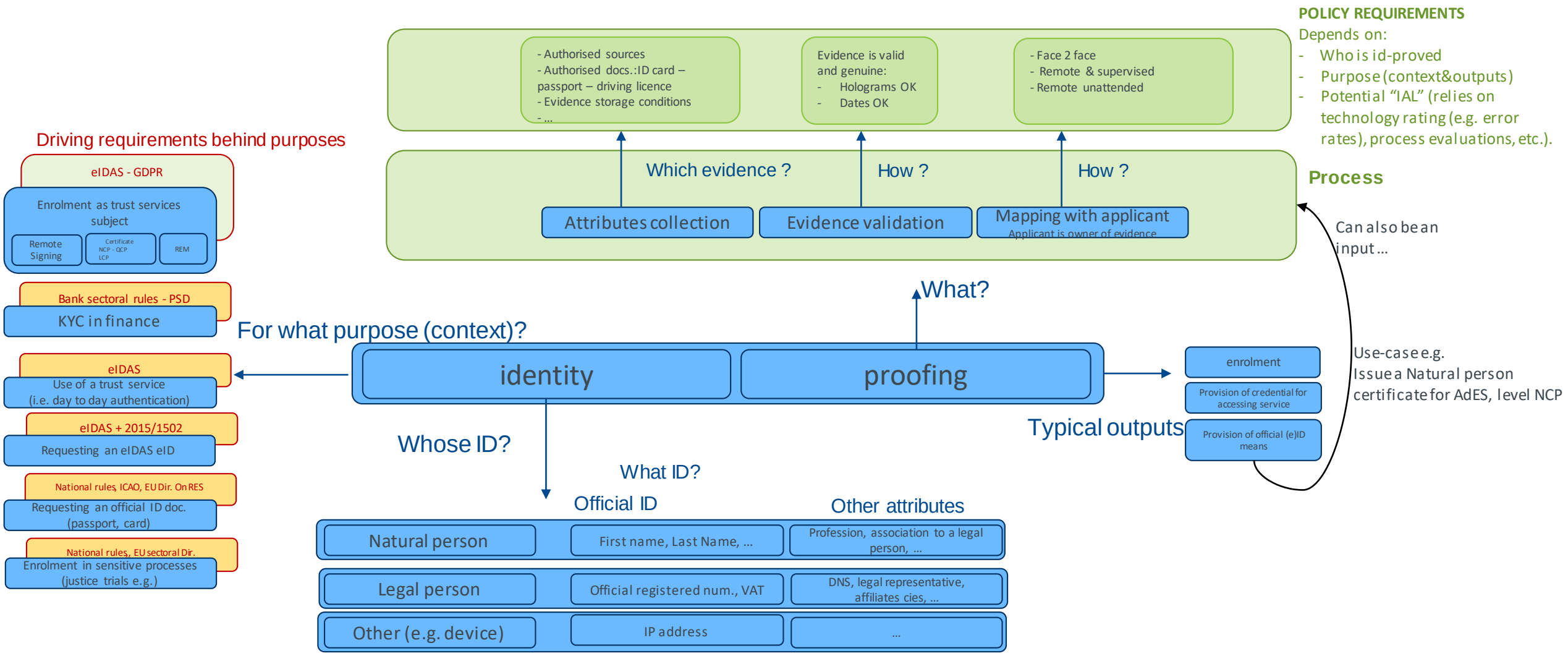
- **ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects. (31/07/2021)**

This document specifies policy and security requirements for a trust service component providing identity proofing of trust service subjects. This can be used for conformity assessment of a trust service provider which includes this service component as part of its service or can be used for conformity assessment of a specialized provider of identity proofing supporting other trust service providers. The document specifies best practices for security supporting different technological approaches, and possibly for different assurance levels.

- ID proofing is NOT a trust service by itself (up to now), but a trust service component
- An identity proofing service may be used by many different trust services
  - One audit that can be reused for different purposes -> ETSI EN 319 403-1 auditable
- Security and policy requirements
  - Based on ETSI EN 319 401 – common requirements for all trust services
  - Specific requirements for identity proofing (relation with EN 319 411-1 / -2 clauses 6.2)
  - Specific requirements to support qualified trust services (! does not mean the ID Proofing is a QTS)

Note: risk assessment, technologies rating -> out of scope

STF 588 scope : identity proofing, part of the broader identity management lifecycle



Implication of “remote” identity proofing

- Attributes and evidence collection
  - What to collect
  - Type of evidence to be / that can be presented
  - Type of presentation of the attributes
  - Communication channels for remote collection
    - Security measures deployed to protect the integrity of the attribute transmission (e.g. end-to-end encryption)
    - Conditions when ID attributes not remotely presented by the applicant but obtained from a third party independent of the applicant (e.g. LoA, authentication, etc.)
- Attributes and evidence validation
  - Determination that the evidence is genuine (issued by recognised independent/authoritative sources)
  - Determination that the ID attributes are valid (not expired, not revoked)
    - Specific conditions for validation of security features when presented on line – remotely transferred
- Mapping (binding) with applicant
  - Face-to-face
  - Supervised remote (e.g. video interview)
    - Conditions on communication channel
    - Specific conditions on personnel in charge
  - Full-remote (unattended automated)
    - Specifications on communication channel
    - Conditions on the authentication level, other (proof of liveliness)


ETSI
The Standards People